

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
22 September 2005 (22.09.2005)

PCT

(10) International Publication Number
WO 2005/088900 A1

(51) International Patent Classification⁷: **H04L 9/30**

(21) International Application Number:
PCT/JP2005/004852

(22) International Filing Date: 11 March 2005 (11.03.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
2004-074739 16 March 2004 (16.03.2004) JP

(71) Applicant (for all designated States except US): MAT-
SUSHITA ELECTRIC INDUSTRIAL CO., LTD.
[JP/JP]; 1006, Oaza Kadoma, Kadoma-shi, Osaka,
5718501 (JP).

(72) Inventors; and

(75) Inventors/Applicants (for US only): NAKANO, Toshi-
hisa. OHMORI, Motoji.

(74) Agents: NAKAJIMA, Shiro et al.; 6F, Yodogawa
5-Bankan, 2-1, Toyosaki 3-chome, Kita-ku, Osaka-shi,
Osaka, 5310072 (JP).

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN,
CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI,
GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG,
KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG,
MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH,
PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, TM,
TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM,
ZW.

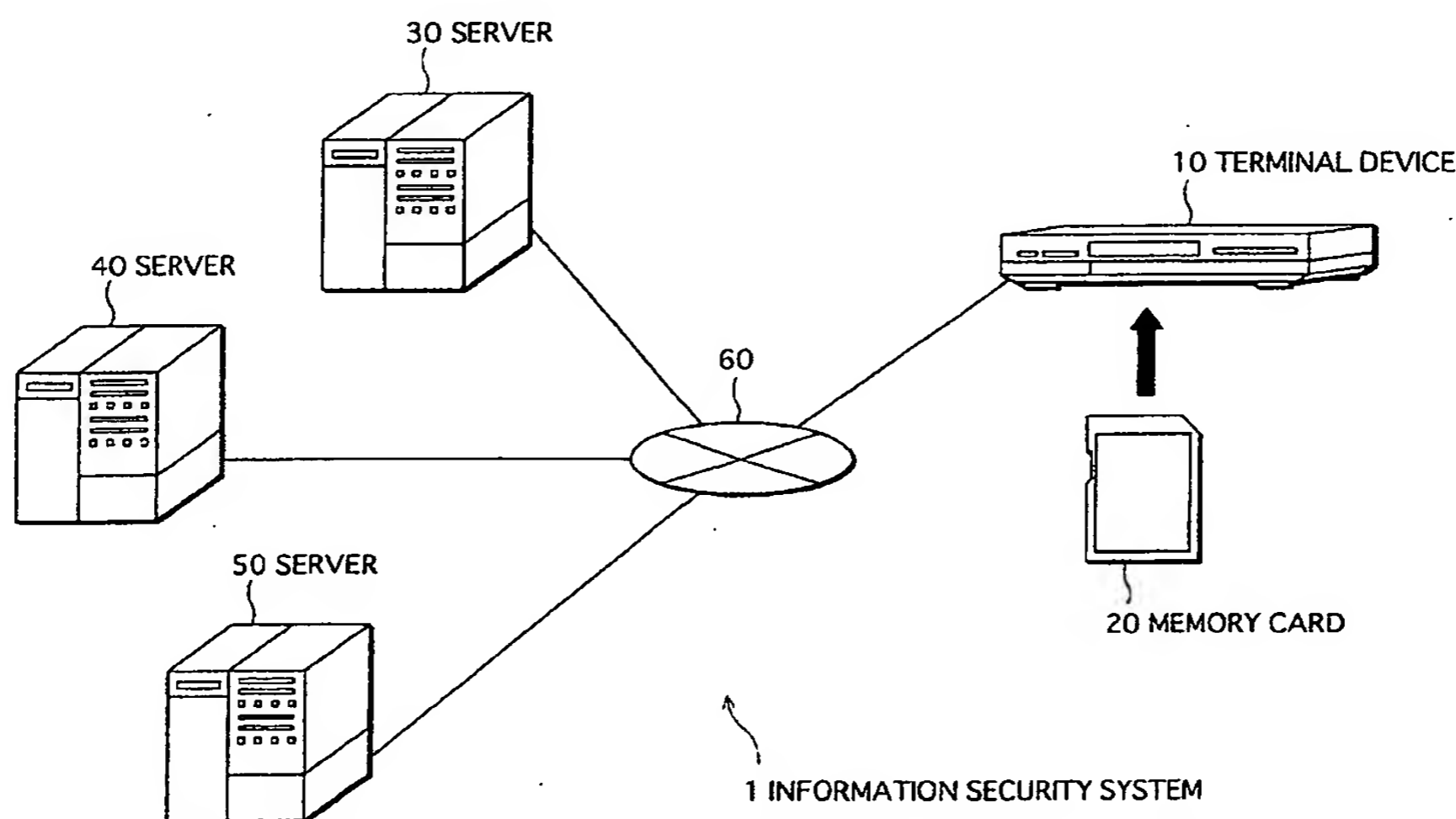
(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),
European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI,
FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO,
SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN,
GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— with international search report

For two-letter codes and other abbreviations, refer to the "Guid-
ance Notes on Codes and Abbreviations" appearing at the begin-
ning of each regular issue of the PCT Gazette.

(54) Title: INFORMATION SECURITY APPARATUS AND INFORMATION SECURITY SYSTEM



(57) Abstract: An information security apparatus that manages information in a safe and reliable manner based on a complexity of an inverse operation on a set of integers that satisfy a condition. The information security apparatus comprises a private key generating unit operable to generate a private key, a parameter receiving unit operable to receive parameters which respectively determine conditions, and a public key generating unit operable to generate, with use of the private key, public keys from sets of integers that satisfy the conditions determined by the parameters.

WO 2005/088900 A1